




SECURITY DOMAIN MINUTES

Date: December 5, 2002


Attendees


- | | |
|--|--|
| <input type="checkbox"/> Dustin Bieghler | <input type="checkbox"/> Doug Less |
| <input type="checkbox"/> Dawna Cape | <input type="checkbox"/> Bob Meinhardt |
| <input type="checkbox"/> Curt Christian | <input type="checkbox"/> Lora Mellies |
| <input type="checkbox"/> Stephen Derendinger | <input type="checkbox"/> Gail Morris |
| <input type="checkbox"/> Hank Henderson | <input type="checkbox"/> R.D. Porter |
| <input type="checkbox"/> Gail Keisker | <input type="checkbox"/> Pete Wieberg |
| <input type="checkbox"/> Barb Kiso | |

New Business

-  Gail Keisker submitted her resignation to Bob Meinhardt. Her replacement is Hank Henderson, a member of the Social Services Security Team. Gail will remain with the group for the initial 60-90 days in order to transition her responsibilities to Hank.

Old Business

-  Reviewed November 21st Minutes
Minutes reviewed and accepted with the following changes to the Technology Areas.

-  Changes: Security Domain Technology Areas (page 6):
 - ☐ Management Controls
 - ☐ Vulnerability Testing was changed to Vulnerability Assessment
 - ☐ Operational Controls
 - ☐ Security Education / Certification was removed because Education is tied to Awareness and Certification needs to go with Training.
 - ☐ Security Awareness was changed to Security Awareness / Education
 - ☐ Security Skills Training was changed to Security Skills Training / Certification

- Discussion: Technical Controls Technology Area:
 - Technical Controls will need additional review to determine whether some items can be grouped together (e.g., Logical Access Controls).
 - Possible misclassification due to the elimination of the NIST Access Control List.
 - Movement should be based on the level of granularity required. For example, Date / Time Controls might be grouped under Access Controls because they might call for only one compliance; whereas IDS is broad enough to warrant its own Technology Area.
- Recommendations from Bob:
 - The following statement can be utilized as a validation premise for determining whether an item required its own technology area:
“If you can assign compliance to it, it’s a good candidate for its own area”
 - As the process evolves, and an assessment of a given Technology Area indicates that one topic has a group of Compliance Components, it can be bumped to its own Technology Area.
 - The Architecture Structure (e.g., Technology Area) is simply a categorization tool. What’s important to the agencies is the actual document produced, not where it’s located in the hierarchy.

■ Housekeeping

- All future meeting handouts will be sent soft-copy with the agenda. Meeting attendees will be responsible for bringing their own copies. The Facilitator will provide any items not e-mailed prior to the meeting.
- Gail Keisker and R.D. Porter will not be present at the November 19 meeting.

■ Review Technology Areas and priorities

- 60-Day Plan
 - R.D. mentioned the controversy within the ITAB committee on firewall policy and its potential impacts on the Security Domain since it was not set in stone.
 - After R.D. informed the group that OA wanted to issue an edict in order to resolve confidentiality issues (e.g., SAM II), the following topics were discussed:
 - The Sunshine Law does not resolve the issues
 - R.D. example – just because a User has access to information does not give them permission to release that information
 - “Confidentiality” is part of the Privacy Domain, but some items fall under Security’s Information Classification Technology Area.
 - Information Classification Discussion:
 - Lora mentioned the Judicial Department at the federal level has a whole section, within one of their manuals, on classifying information

- Bob agreed with Gail M.'s assessment that the compliance would entail the following items:
 - Determination of who owns the information (i.e., statewide vs. agency-specific information)
 - Agencies should establish their own policies:
 - Identification & classification of information (e.g., private, secret, etc.)
 - Method for educating Users so they are aware of what information can be release under what circumstances and by whom
 - Procedure for releasing information to the public
- Group consensus on the current priority list:
 - Incident Response – two compliance components established
 - Virus & Password – low-hanging fruit
 - Information Classification – serves a current need/priority for OA
 - Gateways / Firewalls – analysis and documentation by Domain Committee could assist the resolution of the issue within ITAB

Architecture Blueprint Template Population

Discipline Templates

Management Controls

- Definition: “Management Controls are techniques and concerns, normally addressed by management, regarding the organization’s computer security strategy. It includes the mitigation of risk within the organization.”
- Rationale: Addresses security within a business context
- Benefits: Trust, continue business flow, provide guidance
- Boundary Topics: Add Life Cycle Management and change Certification and Accreditation to System Certification and Accreditation
- Standard Organizations: ISO was added
- Government Bodies: NSA, FBI, Department of Homeland Security
- Stakeholders: Executive Management – Department Director, CIO, CFO, etc.
- Roles: Decision makers; administrative authority

Operational Controls

- ❑ Definition: “Operational Controls are procedures implemented and executed by people, as opposed to systems, to improve the security of a system or group of systems. They often require technical or specialized expertise and may rely upon management activities as well as technical controls.”
- ❑ Rationale: Improve the security of a system or group of systems.
- ❑ Benefits: Standardization; structure; behavior; individual responsibilities
- ❑ Boundary Topics: Remove Personnel Security. It was listed under NIST as “operational” but was classified by the group as a Technology Area under the Management Controls Discipline.
- ❑ Standard Organizations: ISO and SANS (System And Network Security) were added; NIST was changed to specify the Computer Security Resource Center.
- ❑ Government Bodies: HIPPA, DOT, local government
- ❑ Stakeholders: System Administrators; security officers; facility managers
- ❑ Roles: Implementers

Technical Controls

- ❑ Definition: “Technical Controls are security controls executed by computer systems, as opposed to people. The implementation of technical controls requires significant operational consideration and should be consistent with the management of security within the organization.”
- ❑ Rationale: Automated security control that improves system security
- ❑ Benefits: Standardization; efficiency; trust; interoperability; connectivity; ability to perform functions that can’t be executed by people
- ❑ Boundary Topics: Spelling error on “Controls”
- ❑ Standard Organizations: ISO and SANS were added
- ❑ Government Bodies:
- ❑ Stakeholders: Network Administrators, CIT, CIS, etc
- ❑ Roles: Technical personnel

Technology Area Template

Incident Response

- ❑ Definition: “Incident Response capability is a combination of technically skilled people, policies, procedures, and techniques that constitute a proactive approach to handling computer security incidents.
- ❑ Rationale: Provides a consistent approach to handling security incidents.
- ❑ Benefits: Consistent method of evaluation and associate metrics; decrease spread; minimize damage; fulfills risk mitigation; limits impacts; items listed on compliance document
- ❑ Keywords: Incident response; incident reporting; intrusion detection; exposure vulnerability; INFOCON; attack; incident impacts

Compliance Component Templates

Template Changes

- ❑ Change template title to “Compliance Organization”
- ❑ Group or reorder rationale, conditional use, migration strategy, and impact position statement (to identify as sub-part of classification)


Incident Response Reporting

- ❑ Description: Add bullets from the DIS document.
- ❑ Benefits: promotes awareness of incidents; allows for monitoring; builds knowledge base – collecting the right information enables the creation of useful reports (big picture/patterns); standardization
- ❑ Standard Organization: Add Gail Wekenborg name/address contact information
- ❑ Government Body: Replace DIS portion with ITAB information
- ❑ Rationale: Change to “Currently the active plan and procedures authorized by Information Technology Advisory Board”

Incident Risk Level Assessment, and Countermeasures (INFOCON)

- ❑ Name changed to remove “INFOCON” and add “Awareness” – *Incident Risk Level Awareness, Assessment, and Countermeasures*
- ❑ Discussion was held on how this compliance differs from the Response Reporting component. Both are based on ITAB authorized documents. The former addresses reporting only, with comments made that the “Incident Response Plan and Procedures” title is misleading. This compliance addresses those items outside of straight reporting – awareness of incidents, assessments of level, and actions that can be taken. Some reported incidents do not require a change in INFOCON level.
- ❑ Incident Reporting is strictly “reactive” while the INFOCON-based compliance is mainly “proactive” with some reactive elements.
- ❑ Gail M. provided Dawna Cape with the Executive Summary that corresponds to the INFOCON document.
- ❑ Finalization of INFOCON component tabled until the December 19 meeting.

Technology Scans

 Domain Focus will be on Products and/or Compliance Components that are currently being used by the State. Members will look at their own agencies and, as a group, cover those agencies not represented on the committee – through conversations at ITAB Security Committee meetings or other means.

 Due to time constraints, group elected not to conduct the in-session activity.

Homework



Technology Scan Worksheet

- Worksheet is not an official component of Blueprint, but serves as a guideline of “what to think about” when conducting the technology scans. It is a tool for capturing the information that will populate the Product / Compliance Component templates.
- Completed worksheets should be brought to the December 19th meeting, with a copy for Dawna Cape / Doug Less. A soft copy should also be send to Dawna.



Technology Area Definitions

- A preliminary list of definitions was distributed. The committee was tasked with reviewing the list and suggesting any revisions or additions.



Architecture Blueprint item approval

- Blueprint items (e.g., Incident Response Discipline template) will be e-mailed to group for approval. A packet of Blueprint items will then be compiled for submission to the Architecture Review Committee (ARC).

Action Items



Domain Committee

- Review completed templates and Technology Area definitions. Submit comments to Dawna. **December 16, 2002**
- Technology Scan worksheet for Password Policy Controls (compliance) and Virus Detection and Elimination (product). **December 18, 2002**



D. Cape / D. Less

- Update and distribute the Security Domain contact list and meeting handouts. **December 6, 2002**
- Revise and distribute minutes from Nov. 21, 2002. **December 12, 2002**